Security Certification – A critical review

Ragnar Schierholz
Industrial Software Systems
ABB Corporate Research
Segelhofstr 1k
5405 Baden-Daettwil, Switzerland
ragnar.schierholz@ch.abb.com

Kevin McGrath
Industrial Communication
ABB Corporate Research
Bergerveien 12
1375 Billingstad, Norway
kevin.mcgrath@no.abb.com

Keywords: security, assurance, certification, economics, transaction cost, principal agent, industrial, automation, control, system, iacs

ABSTRACT

Security for industrial automation and control systems (IACS) is a much discussed topic for several years now. Certification of security properties of products has been gaining rising attention in the more recent past. We analyze security certification from an economic background and take a look at how security certification initiatives in the enterprise system domain have performed in the past. From this analysis, we extract a number of critical elements which have lead to failure of certification initiatives and check whether and how the current security certification initiatives address these pitfalls.

1 INTRODUCTION

Security for Industrial Automation and Control Systems (IACS) has become a much discussed topic in the recent past. Despite the lack of solid data on incidents and attacks available for research and still comparatively few publicly known vulnerabilities in IACS, there is common agreement among the experts that IACS need to better address security [1,2,3,4,5]. Regulations such as NERC CIP reflect this need and international standards such as ISA 99/IEC 62443 or IEC 62351 as well as industry organizations' guidelines and requirements specifications such as the WIB Security Requirements for Vendors are trying to help the industry achieve better security levels [6]. In particular, these standards attempt to address the specific needs of IACS as opposed to enterprise IT systems [1,3,6].

Security properties of software products or systems (including IACS systems or components) are hard or even impossible to observe during their procurement. In order to ease the process and to increase transparency, several actors in the industry have started certification programs, which certify certain security-related properties of products and systems. There are programs based on proprietary specifications, there are programs based on relatively open specifications, there are programs addressing individual device's stack robustness, there are programs addressing functional security requirements and there are programs addressing development and support processes. So far, there is a lot of confusion about these different programs and their contribution to the automation industry.

In this paper, we attempt to shed some light on the fundamental concepts behind security certification primarily from an economic perspective, not so much a technical one. First, in section 2 we outline the background of standardization and certification in general and relate that to the context of security in particular. In section 3 we explain the fundamental concepts of security certification, look at experiences from other fields and briefly outline how the current security certification programs in the automation industry work. In section 4 we analyze these current programs with regard to the fundamental concepts and the experiences. Finally, we conclude the paper in section 5.

2 BACKGROUND

2.1 SECURITY STANDARDIZATION

The automation industry is strongly dependent on standards. This has various reasons and serves various goals. Probably the most important goals of industry standardization are (adopted from [5][1]):

- Setting a minimum acceptable level of quality for a given scope of a standard (both on a technical and organizational level).
- Enabling technical interoperability of products from different vendors.

Compliance with interoperability standards is usually done by testing against reference implementations or test cases which are part of the standard specification. Examples of interoperability standards in the security domain are protocols such as TLS or data formats such as X.509 certificates. In the automation industry, examples are protocols such as the various fieldbuses or OPC. If the specification of the standard is well written and non-ambiguous, the testing and certification of compliance is an undisputed, trivial matter.

However, standards addressing a minimum level of quality, not interoperability, often are less specific and prescriptive – usually on purpose to leave room for differentiation in the market. An example of such a standard is the ISO 9000 series for quality management. Formal testing of compliance with these standards is usually not possible as the standards do not rigorously specify objectively measurable criteria. Instead, auditors offer certification of compliance and this usually involves the auditor's interpretation of the standard. Over time, a common practice of interpretation is usually established in the respective market. In the security domain, examples of such minimum level of quality standards include the ISO/IEC 27000 series for enterprise information security management or the Common Criteria (ISO/IEC 15408) for information technology security evaluation. Examples from the IACS security domain are the ISA 99/IEC 62443 standard or the Process Control Domain Security Requirements for Vendors as published by the WIB.

Despite the fact that some of these standards are not yet final or published and others are only relatively recently published, different efforts have been conducted or are underway to leverage their results already. These efforts include assessments of deployed control systems to derive recommendations to improve the security of the plants [7], but also certification programs to certify

[1] Regulations and corporate standards are not relevant in this context as regulations usually enforce a minimum level of quality and only differ from standards by the regulating authority's capability of enforcement and corporate standards usually are not subject of certification (as it is understood in this paper).

that certain products, systems or organizations comply with the standards [8,9]. The concepts behind the latter will be the focus of this paper.

2.2 MARKETS WITH INFORMATION ASYMMETRY

As all relevant parties in this scenario are economic actors, it makes sense to also take into account economic considerations when looking at information security and certification. Many economic actions are indeed explained by incentives and market mechanisms the actors are exposed to or affected by [10,11,12,13].

Security properties of a software product are a quality dimension which is difficult to assess for an end user prior to purchase, at least not at a justifiable cost. While statistics about past vulnerabilities may be considered an indicator, this would actually imply that most IACS would be rated rather well. This is a typical case of information asymmetry which is commonly considered a condition leading to market failure [14,15,16]. In this situation the market fails to provide optimal resource allocation. Consider a vendor A selling a product with desirable quality features (in this case strong security) and a vendor B selling a product without the desirable features (i.e. with weak or no security). Vendor A cannot reap the benefits of better quality because vendor B has lower costs and can therefore offer his product at a price which is prohibitively low for vendor A. The customer can't tell the difference due to the information asymmetry and thus will buy from vendor B. This initiates a race to the bottom with regard to the desired quality property. This is commonly called a "market for lemons" referring to the seminal paper of Akerlof [14]. Typically, in these kinds of markets, the normal market mechanisms don't lead to an optimal resource allocation (market failure). Several theoretical frameworks exist which explain such market failures and suggest mechanisms to prevent such failures. In the following we'll take a closer look at some of these frameworks.

3 SECURITY CERTIFICATION EXPLAINED

3.1 ECONOMICS PERSPECTIVE

Several mechanisms have been proposed in order to remove the information asymmetry, among them certification of product properties by an independent third party. The benefit of certification by independent third party certifiers can be explained using the transaction costs theory and principal-agent theory from the economics discipline.

3.1.1 TRANSACTION COST ECONOMICS

Transaction cost economics (TCE) go back to Coase and have been much extended by Williamson [17,18,19,20,21,22,23]. They address the organization of economic transactions. TCE postulates that a producer optimizes not only towards production costs of producing a product, but also takes into account the transaction costs of selling the product on the market and similarly a buyer does not only optimize on purchasing costs for a product but also on transaction costs associated with the purchasing transaction. According to Picot et al. an economic transaction can be subdivided into different stages (see Table 1) [24].

Stage	Examples for associated activities and costs
Initiation	identification of transaction partners, e.g. marketing (on the vendor's side) and product/supplier search and comparison (on consumers' side)
Negotiation	consulting and administrative costs for contract closure, coordination costs in specification, delivery planning, etc.
Settlement	costs for product delivery, management of the exchange of products and payments, validation of delivery and payment
Monitoring	monitoring of quality and timeliness of transaction execution
Adjustment	modification of contracts according to changes in requirements

Table 1: Stages of a market transaction (from [24]**, p. 67)**

Typically, in a market situation the actors are impaired in their decision making by limited information availability. This can be hidden characteristics (of the product or service as well as of the supplier), hidden action or information (when the buyer can't monitor or assess the supplier's actions) or hidden intention (when the buyer cannot sanction the supplier's opportunistic behavior). Consequences can be adverse selection due to hidden characteristics (e.g. primarily customers with bad risk properties looking for an insurance), moral hazard due to hidden action/information (e.g. a supplier billing a buyer for inspections that were not done or not necessary) or hold up due to hidden intention (e.g. a supplier increases service rates after the buyer has invested in the product).

3.1.2 PRINCIPAL-AGENT THEORY

The principal-agent theory goes back to Ross and Jensen/Heckling and has been extended by various researchers [25,26,27,28]. It investigates the implications of such information asymmetry and the associated uncertainties or risks. The theory identifies the role of a principal (e.g. a stock holder or a buyer) sourcing a service or product from an agent (e.g. a management team or a supplier) and models the decision situation from the principal's point of view. During the different stages of a transaction, different costs and risks of this agency relation are imposed on both the principal as well as the agent. The principal-agent theory identifies mechanisms for the governance and minimization of these costs and risks. These mechanisms are signaling, screening and self-selection.

Signalling is a mechanism by which the agent can indicate to the principal that he is able to deliver the desired products/services. Examples for signaling mechanisms are letters of reference or certificates that an applicant shows in his application to indicate to a potential employer that she is a skilled candidate. Three fundamental requirements must be met for a working signaling mechanism:

- For "good agents" the benefits for creating the signal must be higher than the costs of the signal (i.e. the investment pays off).
- For "bad agents" the benefit for creating the signal must be lower than the costs of the signal (i.e. the costs are prohibitively high).
- For the principal, the signal actually has to be a reliable and expressive indicator for the desired property.

Screening is the counterpart of signaling on the principal's side. This summarizes all activities that the principal performs to gather and evaluate the agent's signals.

Self-selection is a mechanism that tries to split the "good agents" from the "bad agents" by setting boundary conditions which motivate the agents to refrain from opportunistic behavior. This is often done by setting up corresponding incentives in a contract. Examples from literature and practice include several examples from the insurance industry [29,30], but also education or law enforcement contracts [30].

Finally, Eisenhardt suggests the establishment of institutions or mechanisms which help in lowering the information asymmetry or differences in interest which are at the root of the agency problems [31]. Examples are contracts based on observable outcome rather on hard-to-observe behavior or information systems that can measure and monitor behavior efficiently. These have to take into account the risk transfer which is implied e.g. by outcome-based contracts where the outcome is partially influenced by factors beyond the control of the agent.

In summary, the transaction cost economics point out frictions (with associated costs) that come with market transactions. The principal-agent theory offers some explanations on how the actors in the market are affected by these frictions and offers some mechanisms for minimizing these costs.

3.1.3 APPLICATIONS IN PRACTICE

Several applications of transaction cost economics and principal-agent theory to industry scenarios are known. Examples include the analysis of outsourcing relationships [32,33], supply chain management [34,35], procurement contracts in general [36] or quality assurance in construction engineering [37]. Of particular interest are the adverse selection and moral hazard problems that appear here due to information asymmetries as well as the mitigation mechanisms such as self-selection and signaling. Schlaak et al. [32] focus specifically on security aspects in outsourcing relationships and the externalities that materialize here.

Nellore [38] argues that validation of specifications can also be done using contracts (even in scenarios with complex specifications and where failures can easily lead to loss of life or other similarly dramatic consequences) based on examples from the aircraft industry. Rice [39] provides an in-depth analysis of multiple mechanisms for achieving stronger software security such as regulation (analogous to the car safety rating in the U.S.), liability legislation, certification (of software engineers, the software development process and of the software itself) or third party assessments and standardization. Eventually Rice points out several weaknesses and strengths of each of these approaches, but unfortunately doesn't come to a final conclusion but calls for a broader discussion.

Obviously, security certification can be viewed as a signaling/screening mechanism. As Rannenberg [40] points out, originally the idea of security certification has been initiated by users and procurers

(particularly the U.S. military and government), hoping to ease the procurement process (while in the industrial automation domain it has been introduced by certification providers). However, there are multiple points often criticized about security certification and the criteria against which certification happens, among them are lack of publicly accessible, standardized certification criteria and processes, meaningfulness of the results (or rather lack thereof) and cost of certification. Section 3.2 briefly discusses the history of security certification and outlines strengths and weaknesses of the existing approaches from the non-industrial industries.

However, as the applications of economic theories on outsourcing, supply chain management or procurement quoted above already showed, certification is not the only mechanism that can help to fix the problem. Typically, these analyses come to the conclusion that proper incentives in the contracts can mitigate the risks (i.e. self-selection mechanisms), e.g. by defining liability clauses or payment based on outcome (e.g. in the procurement contracts or in liability legislation). Almond [41] specifically analyzes liability options of COTS and custom-developed systems (custom-developed being a system where the purchaser defines requirements and suppliers can bid for the project). Given their nature control system projects qualify as custom-developed systems, as they are procured to individual requirements and have a specific implementation phase (engineering and commissioning). Almond further suggests that the purchaser explicitly defines security properties in the requirements and asks for proof of a proper security organization on the supplier's side, incl. a manager position with security responsibilities (and sufficient resources), appropriate security policies or clearly defined security responsibilities (again including sufficient resources) in the development teams. For the implementation phase, Almond recommends that the purchaser's security team and the supplier's security team collaborate closely, including collaborative security assessments and security checks of the planned operations model (processes and responsibilities). This way "the security-savvy buyer will create an environment where business for security deficient vendors will dry up and only organizations which provide secure, flaw-free (or at least 'flaw-fewer') applications will find work" [41].

3.2 HISTORY OF SECURITY CERTIFICATION

As the analysis above shows, the market for secure software has issues of asymmetric information, which can be addressed using mechanisms suggested by economic theories and the certification of security properties can be considered such a mechanism (signaling). This has been applied in the field of software security already for several years. Thus, we now look at the experiences that industries other than the control systems industry has made with such certifications. In this effort we extend the analysis already published by Anderson/Fuloria [13].

3.2.1 TCSEC / ORANGE BOOK

Probably the first major initiative to certify security properties of software products has been the Trusted Computer System Evaluation Criteria (TCSEC) – commonly referred to as the Orange Book. It was initially issued in 1983 by the U.S. Department of Defense as a mandatory requirement in the procurement of information systems. It defined basic requirements for the evaluation of the effectiveness of security controls in those products. Certification was performed by the National Computer Security Center – a division of the NSA. Certification was a lengthy process, involving in-depth analysis by the NSA experts, entry costs were high and for entry a government agency had to sponsor the application for certification. The certification process lead to the system under evaluation

being classified according to a scheme of different security classes – higher security rating required more and stronger security features. The Orange Book system can be characterized by the following properties:

- It was dominated by a relatively powerful buyer (the government), which created a market for certified products.
- The buyer was heavily involved in the certification process, which lead to transparency of the process both with regard to the compliance criteria as well as the rigor of compliance checking and to an alignment of incentives and interests as the evaluator bore the cost of failures of the evaluated system.
- The certification process consumed extensive resources for intensive checks which lead to good results in security improvements – but at high costs.
- The certification process took a long time which lead to certified products lagging behind technology development.

The certified security class depended on the technical security features and thus class of requirements the system met.

3.2.2 ITSEC / COMMON CRITERIA

In 1990, the "Information Technology Security Evaluation Criteria" (ITSEC) were introduced by the governments of Germany, the UK, France and the Netherlands for use in the European Union, which was further encouraged by the 1991 release of the revised version by the European Commission. The ITSEC later evolved into the Common Criteria (CC) which was adopted as an international standard (ISO/IEC 15408).

The CC differs from the Orange Book in several aspects, most notably they do not directly specify technical security features that a system under evaluation has to offer. Instead they employ the concept of a Protection Profile (PP) which is usually defined by a user group and describes security requirements of a scenario relevant to that user group. Additionally, there is the concept of a Security Target document (ST) in which the product vendor defines the security properties and may refer to a set of PPs. Furthermore, there are Security Function Requirements (SFRs) which define functional security requirements comparable to those mandated by the Orange Book. However, the CC does not mandate any SFRs. There are dependencies between SFRs, e.g. limiting access according to roles depends on capability to define roles). Finally, the CC defines the concept of Security Assurance Requirements (SARs) which describe requirements for the development process used to develop the system under evaluation (e.g. managed source code repositories or specific testing procedures). PPs or STs may refer to SFRs and SARs to describe their requirements.

The product is then evaluated against the requirements set out in the ST or PP as chosen by the vendor. The evaluation does not discriminate different levels (called evaluation assurance levels, EAL) by stronger technical requirements but by the depth and rigor of the evaluation. That is, a higher EAL does not mean more security features, but more rigorous evaluation to more depth. Finally, the certification (except for the highest assurance levels) is not performed by the buyer itself, but by licensed evaluators (called Commercial Licensed Evaluation Facility – CLEF). Thus, the CC can be described with the following characteristics:

- It was initiated by a relatively powerful buyer (the governments in the EU), which created a market for certified products. It is now used by a huge number of organizations which has enlarged and diversified the market significantly.
- The buyer is not involved in the certification process, which leads to intransparency of the process both with regard to the compliance criteria (defined by the vendor) as well as the rigor of compliance checking (under control of the CLEF) and a misalignment of incentives and interest as the evaluator is not liable for the failure of evaluated systems. Furthermore, largely leaving out the buyer from the process removes the operational context of the system from the certification, violating the requirements as set forth by Eloff/Solms [42]and Goertzel et al. [43].
- The cost of the certification process depends on the EAL and the way the CLEF actually performs the evaluation, which leads to significantly decreased costs but also to different incomparable certificates (due to variances in the rigor applied by CLEFs) and a race to the bottom as vendors have an incentive to get a certification at the CLEF with the lowest price – driving out the CLEFs which spent more resources on more rigorous evaluations.
- The certified EAL depends on the rigor of the evaluation process and thus doesn't say anything about the technical level of security provided. Generally, certified products are marketed with the achieved EAL, but the technical details such as protection profile(s) and Security Target are not mentioned. This strongly limits the meaningfulness of Common Criteria certificates as history shows that vendors can choose protection profiles or security targets with unrealistic limitations (e.g. certifying a client workstation operating system with a diskless workstation profile). Notably, there is no proven correlation between strong security properties of products and certification achieved. Instead, there are examples of products which have achieved relatively high EAL certification, but later showed significant number of vulnerabilities [44].

In all fairness it should be noted that the designers of the CC did foresee the potential problem of CLEFs competing on price only and thus entering a race to the bottom concerning the rigor of evaluations. To mitigate this risk, national authorities regulate the CLEFs and can revoke their license. However, in practice it has not been observed that a license has ever been revoked [13].

3.2.3 ISO/IEC 27000

The ISO 27000 series is set of standards for enterprise information security which also dates back originally to a government initiative – the British standard BS7799 targeting the secure operation of government information systems. ISO/IEC 27000 differs from the approaches described above in that it addresses the problem entirely from the operational side. The ISO/IEC 27000 standards consist of a part addressing the security program (called Information Security Management System, ISMS) which an enterprise should operate (ISO/IEC 27001). In short, this begins with defining a security policy, defining the scope of the ISMS, performing a risk assessment, deriving mitigation plans and accepting residual risks. This is designed as an iterative, continuous process – called the Plan-Do-Check-Act (PDCA) cycle. Mitigation planning is encouraged to pick security controls from a part describing security controls – both technical and organizational ones (ISO/IEC 27002). An organization can be certified against ISO/IEC 27001 (which contains a normative annex listing security controls from ISO 27002).

Further parts complement the first two, but certification against those is not possible. ISO/IEC 27003 provides guidance on the processes of the PDCA cycle, describing the activities in a workflow style (defining activities, their objectives, their inputs, guidance on performing them and their output).

ISO/IEC 27004 provides guidance on how to setup metrics and measurements to measure the effectiveness of the ISMS and the security controls. ISO/IEC 27005 provides further guidance on information security risk management. Finally ISO/IEC 27006 defines requirements for auditing and certification against ISO/IEC 27001. ISO/IEC 27011 adopts the ISO/IEC 27001 requirements to the specific context of the telecommunications industry. Further refinements of and guidance on this standard are published as ITU standards. Finally, ISO/IEC 27033 part 1 provides guidelines for network security (both organizational and technical) and is planned to be complemented by further parts.

As said above, the target of certification according to ISO/IEC 27001 is primarily the organization using the information system, only secondarily the information system itself (as far as system support for the selected controls is necessary). Audits and certification are performed by private companies. Generally, ISO/IEC 27000 has reached a wide adoption in the enterprise security community. It can be described with the following characteristics:

- It addresses the organization using specific instances of information systems, not the generic software products themselves. While this ensures that the security assessment is context-specific, by design it does not give the buyer of information systems guidance on which products to select. Therefore it doesn't address the transaction cost of information systems procurement, but rather those of the procurement of services based on information systems (e.g. online shopping or IS outsourcing customers can select certified service providers).
- It was initiated by a large community, which created a large and diverse market for certification. For many organizations, ISO/IEC 27001 certification is a mean to demonstrate due diligence concerning information security.
- The system operator is not only heavily involved but the main target of the certification process, which leads to transparency of the process both with regard to the compliance criteria (defined by the system operator according to its own risk assessment) as well as the rigor of compliance checking (being a collaborative process with the auditor). However the main benefit of the ISO 27000 enterprise certification in terms of transaction costs is the system operator's customer, which again is not involved and thus intransparency remains a problem. A misalignment of incentives and interest is still possible as the auditors compete on certification costs and success and are not liable for potential security incidents (e.g. a customer can't hold an auditor liable if he relied on certified online shop system but his account there was later broken into and misused).
- The cost of the certification process depends on the way the auditor actually performs the evaluation. Even though the requirements and guidelines from ISO/IEC 27006 are meant to limit this discretion, similar to CLEF regulation in CC. However, also here the authors have no knowledge of an accreditation having ever been revoked. Furthermore, accreditation is not required to certify against ISO/IEC 27001, so for assessing the quality of a certificate, a user has to inquire about the issuing auditor (which may not be known to him).
- There are no levels of certification, an organization either passes an ISO/IEC 27001 audit/certification or it fails.

3.2.4 SHORTCOMINGS OF EXISTING SECURITY CERTIFICATIONS

As seen above, most known certification programs have their weaknesses. Unfortunately, all of these factors significantly violate the criteria for suitable signaling mechanisms: a "bad agent" can look for a cheap, meaningless certificate when there are no commonly accepted standards, while a meaningful certificate imposes prohibitively high costs on a "good agent" (hidden information leading to adverse selection and hidden action leading to moral hazard). Looking a bit closer, we find several categories of issues:

- Certification criteria

  The certification only is of value as a signaling mechanism, if the criteria actually represent the desired property of the certified product, i.e. whether they are meaningful or not. A buyer needs to be able to assess whether the criteria match his needs. Usually this can only be achieved if the criteria are transparent to the buyer or even publicly available. However, the challenge remains to create a meaningful set of criteria applicable to a broad enough number of buyers to create a sufficient market for certified products.

  Eloff/Solms [42] address the aspect of meaningfulness and come to the conclusion that security of IT systems is dependent on both operational processes in using and managing the IT systems as well as product security. Similarly, Goertzel et al. [43] note that "Software security is a dynamic property – software that is secure in a particular environment within a particular threat landscape may no longer be secure if that environment or threat landscape changes or if the software itself changes." Therefore a meaningful security certification must address the product/in its context of use – incl. the operational processes and the environment it is operated in.

  Generally, testing a given product for vulnerabilities can only produce relatively short-lived test results, as attackers and security researchers continuously discover new ways of attacking systems and vulnerabilities in components used in products and systems (i.e. operating systems and applications). Thus the test cases for certification have to be updated very frequently and for a product that has passed certification last month, today there may be a dozen known vulnerabilities and exploits.

- Race to the bottom

  The buyer usually is liable for the risk resulting from insecure systems. If several certification authorities compete, this means the certification they can provide is identical or at least substitutable. Thus, the only factor they can compete on is the price. Thus, vendors will primarily choose certification authorities by the price of the certification. As the certification authorities are not liable for the risk associated with their action, they have an incentive to decrease their cost to be able to offer the lowest price and to outbid competition. This leads to lax certification criteria or lax evaluation of those criteria (depending on where the certification authority has the flexibility). As the analysis above shows, so far governing mechanisms for rigorous evaluations such as the licensing of certification authorities under national regulation have failed in practice [13].

- Adverse selection

  The race to the bottom also has another side-effect on the value of the certificate. Not only will the rigor of evaluation go down over time, the low price makes it cheaper for a rogue vendor to obtain certification for a product which doesn't hold the desired properties than to redesign the product to build-in the desired property. This leads to adverse selection, where only those vendors obtain certification which can't establish their reputation through other more expensive means (e.g. closely collaborating with important customers on security issues). Edelman [45,46] observes this effect in online shopping sites and the TRUSTe certification.

- Moral Hazard

Certifying products or systems secure may send a wrong message to the market which leads buyers to think that when purchasing a certified secure system, their job is done. As pointed out earlier, the security of a system depends on both the system capabilities and on the operational context where those are used [42,43]. An example of this can be observed in the banking industry, where banks transferred the liability of payment card fraud based on security claims of payment card authentication systems, but operated the systems in a lax manner [47]. It should be admitted though that this scenario is less applicable to the control system industry, as the operators of the system usually also have liability for the risk of their operations.

- Lifecycle considerations

  Nowadays it is commonly accepted that the threat landscape is continuously changing and that target systems need to react to this change. One example is the significant number of researchers that search for vulnerabilities in products to which vendors react by publishing updates to their products. A change to the product however invalidates the certificate and therefore requires a re-certification (incl. the time delay and additional cost associated with this). This puts an end-user organization which mandates certified products into the dilemma of either sticking to their policy of using certified products only versus fixing a known issue in their system. Similarly, product vendors are in a dilemma. They have to choose between fixing a a known issue and loose certification for the latest release of their product (at least until re-certification can be achieved) or not fixing a known but maintaining the product certification (which again points out the limited meaningfulness of product certification).

3.3 CURRENT AND UPCOMING APPROACHES IN INDUSTRIAL AUTOMATION

Several certification programs exist today, some more successful than others. The following is a list of such programs that will be described in this section

- WST Achilles Communications Certification (ACC)
- WST Achilles Practices Certification (APC)
- Exida's Integrity Certification
- Mu-Dynamics MUSIC Certification
- ISCI ISASecure EDSA Certification

In general, the certification programs are used as a means to communicate an acceptable security level from different vantage points, Table 2 summarizes at an abstract level what each can communicate to stakholders.

Program	**What it communicates?**
ACC, MUSIC, ISASecure ESA CRT	Communicates an acceptable level of stack robustness
WIB/APC	Communicates an acceptable level of organizational preparedness

ISASecure EDSA FSA and SDSA	Communicates an acceptable security functionality and acceptable secure development practices

Table 2 – What it communicates?

It is important to be aware of the dangers of certifying a device, system or product line. Having a security-related certificate, may send an incorrect message to stakeholders, such as a PLC been labeled "certified secure" but at same time vulnerable where evaluation platforms were unable to test, due to limitations on the tool side. Take the example of a certified PLC, which is vulnerable to an attack vector not yet covered by the stack communication certification program.

Security-related certificates carry the risk of introducing a false sense of security, even if unintended. Moreover a race to the bottom issue may even lead to improper test execution during certification with at least some certifiers, if not countered by appropriate mechanisms (who guards the guards).

At the same time the value of these programs should be acknowledged. The programs have raised awareness of security.

3.3.1 WURLDTECH ACHILLES COMMUNICATIONS CERTIFICATION

The most widely spread certification, measured by the number of certifications, is the ACC Program provided by Wurdtech Security Technologies (WST). Although a proprietary methodology is used, the said certification program has become the de-facto for the industry today. This is clearly shown by the number of certifications to date, when compared to Exida (achieved through Wurldtech's evaluating platform), MuDynamics and ISASecure (to be operational in second half of this year) certification programs. This is further shown in Figure 1. All certifications considered in Figure 1, represent a device passing tests (covering traffic storms and attack vectors) relating to core protocols found in layers 2-4 of the OSI model.

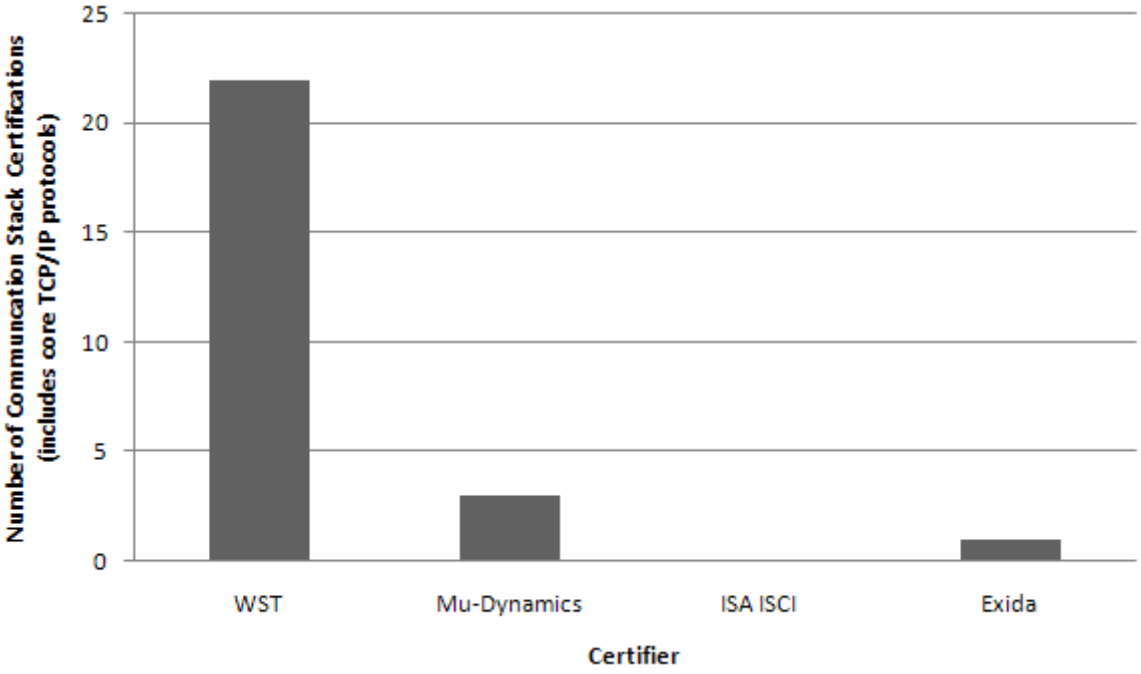

Figure 1 – Number of Communication Stack Certifications (over a 3-year period)

The certification program applies the categorized component model proposed by ISA 99 derived requirements task group, that is it distinguishes embedded devices, network components, host devices and control application. The available certification levels are shown in Table **3**, where Level 1 is widely used.

Certification requires the use of a proprietary third-party control system evaluation platform named the Achilles Satellite Unit. The unit carries out the following test cases; Negative testing (Grammar-based test generation) iterates through the protocol to identify various implementation weaknesses/ vulnerabilities, e.g. coding errors (buffer overflow, and format string bugs). Traffic storms simulate denial-of-service attacks, in an attempt to exhaust resources, such as network, bandwidth, CPU time, or memory. Known vulnerability testing which is an automated process using appropriate scanning tools and techniques to identify existing weaknesses and security holes.

Name	Detail
Level 1	Widely used protocols found in layers 2-4 of OSI model
Control	Protocols specific to industrial control
Proprietary	Closed protocols that are specific to a vendor
Other	Protocols that do not belong to the in the above categories

Table 3 **– ACC certification levels**

The Wurldtech ACC program can be described with the following characteristics:

- It was initiated by WST, who created a market for certified products. It is now used by many IACS vendors, as part of the development process or at the request of customers. Through a partnership with Exida, WST have licensed out their certification service.
- The buyer is not involved in the certification process, which leads to intransparency of the process with regard to the the rigor of compliance checking and a misalignment of incentives and interest as the evaluator is not liable for the failure of evaluated systems. Furthermore, largely leaving out the buyer from the process removes the operational context of the system from the certification, violating the requirements as set forth by Eloff/Solms [42]and Goertzel et al. [43]
- The cost of certification process is influenced by the desired certification level and the way the evaluator performs the evaluation. The evaluator can either be an authorized body or the vendor requesting the certification. In the latter case, test reports are independently verified by the certifier. In this instance, the cost of certification is significantly less to the certifier, but additional costs such as purchasing of the evaluation platform and the associated labor required to perform certification needs to be considered. A certificate is only valid for the tested version of a product, i.e. fixes for discovered vulnerabilities void the certificate, even though one would assume that security is improved by the fix.
- Various certification levels are provided by WST, information on this in Table **3**. The certified product depends on passing a suite of tests provided by the evaluation platform. Providing more information to stakeholders on test coverage for each protocol would give more value to the certificate. The levels of certification are shown in Table **3**, the higher the certification level the more robust control communication protocols are.

3.3.2 WURLDTECH ACHILLES PRACTICE CERTIFICATION

Earlier this year, WST launched a new certification category, called the Achilles Practices Certification program. This certification is derived from WIB Process Control Domain - Security Requirements for

Vendors [48]. So far, Wurldtech is the only accredited certification authority that can certify against the WIB requirements, but the WIB has stated that accreditation shall be open to other certification bodies. The Achilles Practice Certification (APC) does not address a product, but rather a product vendor and/or system integrator. It defines requirements on the organizational policies and procedures as well as organizational responsibilities. These requirements are categorized according to different process areas. An organizational process area defines general requirements both product vendors and system integrators should address (e.g. providing a central security contact, have policies in place). A second process area specifies product requirements on a system level (e.g. it mandates system hardening, account management capabilities, etc.). A third process area addresses the system integrator and specifies requirements for the commissioning and maintenance phase of projects (e.g. system hardening, account configuration and management). These requirements basically seem to intend to ensure that the product capabilities defined in the product process area are properly used in a given project. Different levels of certification are planned, based on the System Security Engineering Capability Maturity Model [49]. With these process areas, the APC is very close to the requirements as set forth by Eloff/Solms [42]and Goertzel et al. [43] and the recommendations by Almond [41]. Thus the Wurldtech APC certification can be described with the following characteristics:

- It was initiated by an industry association of buyers (asset owners from different process industries), which could create a market for certified organizations. It is so far only used by a single member of this association though, so the market is not developed fully yet. This may be at least partially due to the fairly recent release of the specification.
- The buyer is not involved in the certification process, which could lead to intransparency of the process both with regard to the compliance criteria (defined by the accredited certification authority and approved by WIB) as well as the rigor of compliance checking (under control of the accredited certification authority) and a misalignment of incentives and interest as the evaluator is not liable for the failure of evaluated systems. However, there are plans for a regulation of certification authorities by accreditation through WIB. It remains to be seen whether the WIB can better control the rigor of certification authorities than the national regulators for CC and ISO 27000.
- The organizational context is addressed via the process area requirements for commissioning and maintenance. However, the certification is not done per project but per organization working on projects. Thus the certification checks whether the organization has policies in place but can't check whether the policies are adhered to in a given project. It remains to be seen how the construct of senior management signed statements can hold up in a liability context.
- The cost of the certification process depends on the compliance criteria and the way the evaluator actually performs the evaluation, which leads to significantly decreased costs but could also lead to different incomparable certificates (due to variances in the compliance criteria and the rigor applied by evaluators). Thus a race to the bottom is possible as vendors have an incentive to get a certification at the authority with the lowest price – driving out the authorities which spent more resources on more rigorous evaluations. Again, this will have to be countered by the accreditation process of the WIB and can only be evaluated seriously once more certification authorities compete.
- The certified level depends on the maturity of the processes in place, that is higher certification levels indicate a more mature organization with advanced policies and procedures in place, which should be able to produce better security.

3.3.3 EXIDA INTEGRITY CERTIFICATION

With the acquisition of Byres Research in 2009, Exida expanded its business to include functional security services. Through this acquisition and a partnership with WST, Exida were able to create a new certification program that would evaluate functional safety, security and reliability. The program is called Integrity Certification [50] and was launched at ISA Expo 2009. Although Exida have Achilles certified one product (Honeywell's Experion Safety Manager), no product line has received the Integrity Certification. The certification program involves evaluation of a product and development process to determine its Safety Integrity Level (SIL) capability and a security assessment based on ISA Security Compliance Institute Embedded Controller Security Assurance (EDSA) test specification. This assessement includes a combination of network stack robustness testing (probably involving the WST Achilles Satellite unit), functional security assessement and a development lifecycle assessment in order to detect and avoid vulnerabilities. The Integrity Certification program would create a one stop shop for safety and security certifications. Given the functional security is evaluation is based on ISCI EDSA test specficiations, the analysis is carried out on section relating to the ISCI ISASecure certification program.

3.3.4 MUDYNAMICS MUSIC CERTIFICATION

Mu Dynamics offers a certification program for industrial devices, called MUSIC Certification [51]. It operates in a similar manner to that of the ACC program; however its acceptance lags behind the latter, with a total of 3 devices certified over a 3 year period. This program requires the use of an evaluation platform, which in this case is the Mu-8000 Service Analyzer [52]. It supports a similar set of test cases as the Achilles Satellite unit. However in saying that, protocol test coverage is not known for these types of tools. For the MUSIC Certification program, the certification levels are shown in Table 4, certified devices have only received Foundation Level recognition. Mu-Dynamics have indicated they are planning to phase out the MUSIC Certification program in favor of the ISASecure certification program, whether that means MuDynamics will seek accreditation to be a certified body or seek recognition of the evaluation platform for the commmunication robustness part of ISASecure EDSA, remains to be seen.

Level	**Detail**
Foundation	Includes ARP, DHCP, IEEE 802.1p/Q, IPv4, TCP, TFTP, UDP
Advanced	Application and control protocol analysis

Table 4 – MUSIC certification Levels

The Mu Dynamics MUSIC certification can be described with the following characteristics:

- It was largely initiated by the test equipment supplier. No clear facts available on why but one can speculate the following motivation, (i) a growing number of customers from the IACS sector, (ii) direct customer request for certification service, (iii) participation in ISCI, (iv) opportunity to expand and grow business.
- The buyer is not involved in the certification process, which leads to intransparency of the process with regard to the the rigor of compliance checking and a misalignment of incentives and interest as the evaluator is not liable for the failure of evaluated systems. Furthermore, largely leaving out the buyer from the process removes the operational context of the system from the certification, violating the requirements as set forth by Eloff/Solms [42]and Goertzel et al. [43]
- The cost of certification process is influenced by the desired certification level and the way the evaluator performs the evaluation. The evaluator can either be an authorized body or the vendor requesting the certification.In the latter case, digitally-signed tests are independently verified by an authorized body. In this instance, the cost of certification is significantly less to the certifying body, but additional costs such as purchasing of the evaluation platform and the associated labor required to perform certification needs to be considered.
- The certified product depends on the rigor of tests from the evaluation platform. A drawback of the certified products is that key device functions were not monitored through the evaluation platform during test and hence could not be a part of the certification process. Recently, Mu-Dynamics have extended the evaluation platform to support the monitoring of key device functions. The levels of certification are shown in Table 4, the higher the certification level the more robust control communication protocols are.

3.3.5 ISCI ISASECURE

The ISA Security Compliance Institute (ISCI) was founded in 2007. ISCI is focusing on integrating security into the product development lifecycle by introducing a conformance testing program. In 2010, ISCI has published parts of the *ISASecure Embedded Device Security Assurance (EDSA)* certification specification [53]. ISASecure EDSA is one of many planned certification programs under the ISCI mandate. The ISASecure EDSA certification program consists of the following parts

- Functional security assessment (FSA)
- Software development security assessment (SDSA)
- Communication robustness testing (CRT)
-

A mapping of certification levels to FSA, SDSA and CRT is shown in Figure 2. A brief description of each follows; The FSA audits the devices security functionality, for example the ability to maintain network resource availability under different conditions, against vendor documentation and the requirements for the desired certification level. The SDSA audits the vendor's software development processes, similar to when a safety-related system has been SIL certified to the software development requirements in IEC 61508. Moreover the SDSA requirements are partly derived from IEC 61508 and

other reference models. This is often seen as problematic, as attacks on security do not occur according to a statistical distribution, as random failures subject to the laws of physics do. The third part of this certification is CRT. This is closely related to existing certifications programs, such as *Achilles Communications Certification* program. A key aspect of both programs is that the critical function, such as the safety loop, must be adequately maintained to achieve certification.

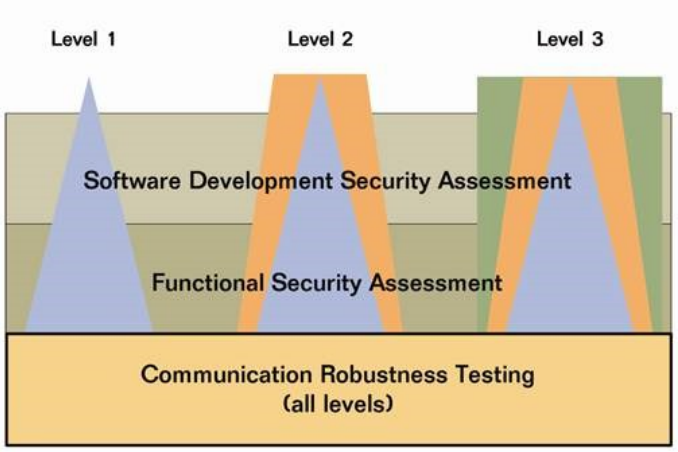

Figure 2 – Certification levels [53]

The ISCI ISASecure EDSA certification can be described with the following characteristics:

- It was initiated by a standards organization, which could create a market for certified products. The standards organization has formed a consortium which includes control system users (asset owners from OGP sector), manufacturers and industry organizations who may be involved in certifying products. Given the recent release of the specification, it is anticipated that the certification program will become operational in the second half of this year.
- The buyer is not involved in the certification process, which leads to intransparency of the process with regard to the the rigor of compliance checking and a misalignment of incentives and interest as the evaluator is not liable for the failure of evaluated systems. Furthermore, largely leaving out the buyer from the process removes the operational context of the system from the certification, violating the requirements as set forth by Eloff/Solms [42]and Goertzel et al. [43]
- The cost of certification process depends on the desired EDSA level and the way the chartered laboratory actually performs the evaluation. The rigor and cost applied by one chartered laboratory should be the same for another. Variances in rigor and cost would aid a race to the bottom scenario as vendors have an incentive to get certification at the chartered laboratory with the lowest price – driving out the chartered laboratories which spent more resources on more rigorous evaluations.
- The certified level depends on the rigor of the evaluation process and the maturity of manufacturer development processes. In order for certificates to be comparable and meaningful, besides requiring consistency for FSA and SDSA audits, test coverage of different CRT tool needs to be considered and its impact on the certificate

4 ANALYSIS

In this section we will summarize the analysis of the current security certification initiatives and point out some elements where we see a danger of mistakes from enterprise system security certification being repeated. Since the certification initiatives are still in a maturing phase, we see this as a constructive criticism, aiming at the improvement of the overall situation in the industry.

- Certification criteria

  In most current certification programs, the certification criteria are not publicly accessible, i.e. they can't be evaluated by subject matter experts for their meaningfulness. Furthermore, buyers seeking a meaningful signaling mechanism have no way of checking the appropriateness of a given certification program for their purposes. Obviously, certification program developers currently are in discussion with individual buyers to market their programs and also disclose the criteria to these buyers. However, this merely shifts the transaction costs from evaluating a supplier to evaluating a certification program and thus at least reduces if not eliminates the economic advantage of signaling. Furthermore, this cannot be expected to be a permanent approach, as the evaluators will need to stabilize their certification criteria to achieve a stable and comparable certificate.

- Race to the bottom

  Most current certification initiatives encourage or at least enable independent evaluators to also setup certification programs under the same framework. While the requirements for certification are defined, the specific certification criteria and the process applied to assess a subject's compliance are not strictly defined not is there a requirement to make them public. This makes the programs susceptible to the "race to the bottom" in which evaluators compete on price and probability of passing.

- Adverse selection

  Limited meaningfulness may lead vendors who take security serious to engage in other signaling mechanisms, e.g. in-depth discussions with buyers in the project specification phase. Especially in a market which is characterized by a low number of large actors on both the buyer and the supplier side where buyers choose a few strategic suppliers for mid- to long-term periods, this may turn out to be a suitable and more cost-effective mechanism. Then certification will be used only by small suppliers or by those who can't convince in individual discussions.

- Moral Hazard

  Using only certified products or systems may lead to a lax attitude towards security in the system operations phase. However, as already pointed out in section 3.2.4, this may be well enough under control in the control system security domain, as the operators of the control systems are largely responsible for the risks associated with the operations. However, buyers need to be aware of the fact that good security in the products and systems can only be a solid basis for secure system operation, but must actually be used and maintained throughout the system lifecycle with an appropriate security organization – both resources and responsibilities as well as policies and procedures.

- Lifecycle considerations

Especially in the control system domain which can be characterized by a low number of overall installed systems with a long lifetime, it is important to also consider lifecycle aspects in the security discussion. Certification programs which only focus on a snapshot of the product's security properties at release time and require a recertification for every minor release don't take this lifecycle into account properly. They entirely ignore the operations phase of the system and – if they impose a meaningful rigor in evaluation criteria and process - cause significant costs which can only be shared across a low number of products instances sold to the market. Instead, certification programs which focus on the maturity of an organization (including the product development, the project engineering and commissioning as well as the operation) can actually cover the entire lifecycle.

5 CONCLUSIONS

We come to the conclusion that while the current security certification initiatives in the industrial automation and control systems domain have some merits, they all have a number of weaknesses in their design which make them susceptible to failure. The industry should learn from the experiences that the enterprise system domain has made with security certification programs and either improve the design of the current programs accordingly or avoid certification entirely and instead choose alternative mechanisms to prevent market failure. Specifically, we believe that the industry should leverage the close relationship which most vendors and buyers have to engage in focused security discussions and develop sound security requirements and mutual confidence in the organizational maturity with regard to security. In some cases, this may lead to the development of meaningful and cost-effective security certification, which could well be based on some of the programs currently available in the market or discussed in the industry. Errors made in this phase of the program design can be costly for the entire industry and hard or impossible to correct in the future. Security requires a holistic approach covering the entire lifecycle including product development, project engineering and commissioning as well as system operation with the specific system's operational context. Cost of certification should be considered, especially their potential to put small suppliers and new market entrants at significant disadvantage. Generally, developing such an approach requires close collaboration of all stakeholders and market actors, including end-users, system integrators and product vendors. We hope that we could contribute to this collaboration with our analysis.

6 REFERENCES

[1] D. Dzung, M. Naedele, T. Von Hoff, and M. Crevatin, "Security for industrial communication systems," *Proceedings of the IEEE*, vol. 93, 2005, p. 1152–1177.

[2] E. Byres and D. Hoffman, "The Myths and Facts behind Cyber Security Risks for Industrial Control Systems," *Control*, 2003.

[3] M. Naedele, "IT Security for Automation Systems," *Industrial Information Technology Handbook*, R. Zurawski, CRC Press, 2004.

[4] E. Byres, J. Carter, A. Elramly, and D. Hoffman, "Worlds in collision: Ethernet on the plant floor," *ISA Emerging Technologies Conference*, Instrumentation Systems and Automation Society, 2002.

[5] R. Schierholz and B. de Wijs, "Cybersecurity in power plants: Still an underestimated problem - How end users and vendors are or should be facing it," *PowerGen Europe*, Amsterdam: Pennwell Publishing, 2010.

[6] M. Naedele, "Standardizing Industrial IT Security A First Look at the IEC approach," *Proc. 10th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 05)*, IEEE Computer Society, 2005.

[7] R. Schierholz, S. Obermeier, L. Guidi, D. Pestonesi, and G. Carpi, "Evaluation of ISA 99 in a Real-World Power Plant Security Assessment," *DHS Industrial Control System Joint Working Group 2010 Spring Conference*, San Antonio, TX: Department of Homeland Security, 2010.

[8] P. Kwaspen and T. Williams, "Functional Cyber Security Best Practices Certification Program: An Update for Industrial Stakeholders," *DHS Industrial Control System Joint Working Group 2010 Spring Conference*, San Antonio, TX: Department of Homeland Security, 2010.

[9] T. Culling, A. Ristaino, K. Staggs, and J. Cusimano, "Role of Product Certification in an Overall Cyber Security Strategy," *DHS Industrial Control System Joint Working Group 2010 Spring Conference*, San Antonio, TX: Department of Homeland Security, 2010.

[10] R. Anderson and T. Moore, "The economics of information security.," *Science (New York, N.Y.)*, vol. 314, 2006, pp. 610-3.

[11] R. Anderson and T. Moore, "Information Security Economics – and Beyond Foundational Concepts," *Information Security*, 2008, pp. 1-26.

[12] R. Anderson and S. Fuloria, "Security Economics and Critical National Infrastructure," *2009 Workshop on the Economics of Information Security*, 2009.

[13] R. Anderson and S. Fuloria, "Certification and evaluation: A security economics perspective," *2009 IEEE Conference on Emerging Technologies & Factory Automation*, IEEE Comput. Soc. Press, 2009, pp. 1-7.

[14] G.A. Akerlof, "The Market for "Lemons": Quality Uncertainty and the Market Mechanism," *The Quarterly Journal of Economics*, vol. 84, 1970, p. 488.

[15] F.M. Bator, "The Anatomy of Market Failure," *The Quarterly Journal of Economics*, vol. 72, 1958, pp. 351-379.

[16] S. Balakrishnan and M. Koza, "Information asymmetry, market failure and joint-ventures : theory and evidence," *Journal of Economic Behavior and Organization*, vol. 20, 1993, pp. 99-117.

[17] R.H. Coase, "The Nature of the Firm," *Economica*, vol. 4, 1937, pp. 386-405.

[18] O.E. Williamson, *Markets and Hierarchies: Analysis and Antitrust Implications*, New York: The Free Press, 1975.

[19] O.E. Williamson, "Transaction-Cost Economics: The Governance of Contractual Relations," *The Journal of Law and Economics*, vol. 22, 1979, pp. 233-261.

[20] O.E. Williamson, "The Economics of Organization: The Transaction Cost Approach," *The American Journal of Sociology*, vol. 87, 1981, pp. 548-577.

[21] O.E. Williamson, "Assessing Contract," *Jounal of Law, Economics and Organization*, vol. 1, 1985, pp. 177-208.

[22] O.E. Williamson, "Transaction Cost Economics: How it Works; Where it is Headed," *De Economist*, vol. 146, 1998, pp. 23-58.

[23] O.E. Williamson, "Transaction Cost Economics and Organization Theory," *Technology, Organization, and Competitiveness: Perspectives on Industrial and Corporate Change*, G. Dosi, D.J. Teece, and J. Chytry, Oxford University Press, 1998, pp. 17-66.

[24] A. Picot, H. Dietl, and E. Franck, *Organisation: Eine ökonomische Perspektive*, Stuttgart: Schäffer-Poeschel, 1999.

[25] S.A. Ross, "The Economic Theory of Agency: The Principal's Problem," *The American Economic Review*, vol. 63, 1973, pp. 134-139.

[26] M.C. Jensen and W.H. Meckling, "Theory of the Firm : Managerial Behavior , Agency Costs and Ownership Structure Theory of the Firm : Managerial Behavior , Agency Costs and Ownership Structure," *Journal of Financial Economics*, vol. 3, 1976, pp. 305-360.

[27] K. Spremann, "Agent and Principal," *Agency Theory, Information, and Incentives*, G. Bamberg and K. Spremann, Berlin: Springer, 1987, pp. 3-38.

[28] S.P. Shapiro, "Agency Theory," *Annual Review of Sociology*, vol. 31, 2005, pp. 263-284.

[29] A. Blomqvist, "The doctor as double agent: Information asymmetry, health insurance, and medical care," *Journal of Health Economics*, vol. 10, 1991, pp. 411-432.

[30] M. Harris and A. Raviv, "Some Results on Incentive Contracts with Applications to Education and Employment, Health Insurance, and Law Enforcement," *The American Economic Review*, vol. 68, 1978, pp. 20-30.

[31] K.M. Eisenhardt, "Agency Theory: An Assessment and Review," *Academy of Management Review*, vol. 14, 1989, pp. 57-74.

[32] B. Schlaak, S. Dynes, L.M. Kolbe, and R. Schierholz, "Managing of Information Systems Risks in Extended Enterprises: The Case of Outsourcing," *Proceedings of the Fourteenth Americas Conference on Information Systems*, Toronto, ON, CA: 2008.

[33] D. Wu and L. Hitt, "Learning in ERP contracting: a principal-agent analysis," *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the*, IEEE, 2003, pp. 217-225.

[34] X. Huans, "Production Strategy in Supply Chain under Asymmetric Information," pp. 2-6.

[35] X.H. Lei and K. Zhang, *Research on the subdivision of transaction cost in supply chain based on analysis of enterprises relation*, IEEE, 2008.

[36] P. Bajari and S. Tadelis, "Incentives versus transaction costs: a theory of procurement contracts," *Rand Journal of Economics*, vol. 32, 2001, pp. 387-407.

[37] X. Chen, L. Ding, H. Luo, and J. Sun, "Research on the Optimal Inentive Contract Considering Contractor's Intrinsic Motivation in the Construction Quality Insurance System," *Proceedings of the Seventh International Conference on Machine Learning and Cybernetics*, IEEE, 2008.

[38] R. Nellore, "Validating specifications: a contract-based approach," *IEEE Transactions on Engineering Management*, vol. 48, 2001, pp. 491-504.

[39] D. Rice, *Geekonomics - The Real Cost of Insecure Software*, Upper Saddler River, NJ: Addson-Wesley, 2008.

[40] K. Rannenberg, "IT Security Certification and Criteria - Progress , Problems and Perspectives," *Proceedings of the IFIP TC11 Fifteenth Annual Working Conference on Information Security for Global Information Infrastructures*, S. Qing and J.H. Eloff, Kluwer, 2000, pp. 1-10.

[41] C. Almond, "Should vendors be liable for security flaws in software?," *Computer Fraud & Security*, vol. 2009, 2009, pp. 4-7.

[42] M.M. Eloff and S.H. Solms, "Information Security Management : An Approach to Combine Process Certification And Product Evaluation," *Science*, vol. 19, 2000, pp. 698-709.

[43] K.M. Goertzel, T. Winograd, H.L. McKinley, L. Oh, M. Colon, T. McGibbon, E. Fedchak, and R. Vienneau, "Software Security Assurance: State-of-the-Art Report," *Information Assurance Technology Analysis Center (IATAC)*, 2007.

[44] J. Shapiro, "Understanding the windows EAL4 evaluation," *Computer*, vol. 36, 2003, pp. 103-105.

[45] B. Edelman, "Adverse selection in online "trust" certifications," *Proceedings of the 11th International Conference on Electronic Commerce - ICEC '09*, New York, New York, USA: ACM Press, 2009, p. 205.

[46] B. Edelman, "Adverse selection in online “trust” certifications and search results," *Electronic Commerce Research and Applications*, 2010.

[47] R. Anderson, "System Evaluation and Assurance," *Security Engineering – A Guide to Building Dependable Distributed Systems*, Wiley, 2008, pp. 857-888.

[48] WIB, "Process Control Domain - Security Requirements for Vendors," 2010, pp. 1-33.

[49] CMU, "Systems Security Engineering Capability Maturity Model (SSE-CMM) V3.0," *Carnegie Mellon University - Software Engineering Institute*, 2003.

[50] Exida, "Professional Services for Control System Security Functional Safety Services : Intersection between Safety and Security," 2009.

[51] Mu-Dynamics, "Mu Dynamics Industrial Control Certification (MUSIC)," 2007.

[52] http://www.mudynamics.com, "The Mu Test Platform," 2010.

[53] http://www.isasecure.org/Certification-Program/ISASecure-Program-Description.aspx, "ISCI ISASecure EDSA Specification," 2010.

[54] NIST, "Requiring Software Independence in VVSG 2007 : STS Recommendations for the TGDC," *Technical Guidelines Development Committee*, 2006.